SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SIXTEEN GOOGLE ACCOUNTS THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 2:21-mj-00224 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Terrance L. Taylor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are

necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

3. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422.

4. As a Special Agent, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the District of Southern West Virginia. I have received training in the areas of child pornography and child

exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography), 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography), and 2422(b) (enticement of a minor) (collectively, the "Subject Offenses") have been committed by TODD CHRISTOPHER ROATSEY ("ROATSEY"). There is also probable cause to search the information described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. On or about August 22, 2021, MediaLab/Kik submitted CyberTip Report 98779073 to the NCMEC CyberTipline. The CyberTip Report was the result of MediaLab/Kik representatives reporting to NCMEC that a Kik profile bearing the username "jsparrow2174" had uploaded eight (8) videos and one (1) image through Kik Messenger. Kik representatives viewed the aforementioned files and found them to contain depictions of prepubescent and pubescent minors engaged in sexual activity. Kik representatives advised the aforementioned files were sent from "jsparrow2174."

9. In Cybertip Report 98779073, MediaLab/Kik reported the following information regarding Kik user "jsparrow2174" uploading eight videos and one image of apparent child pornography between on or about July 13, 2021, and on or about July 16, 2021:

Email Address: ultimatew31@gmail.com

Screen/User Name: jsparrow2174

IP Address: 47.220.40.206 on 08-19-2021 at 21:35:46 UTC

NCMEC Geo-Lookup: Elkview, WV, Suddenlink Communications

10. On or about September 16, 2021, HSI Charleston issued an administrative subpoena/summons to Suddenlink Communications regarding subscriber information pertaining to IP address 47.220.40.206 on July 13, 2021, through July 16, 2021. The information provided by Suddenlink indicated that the IP address was assigned to the Elkview, Kanawha County, West Virginia residence owned by ROATSEY.

11. On October 27, 2021, a federal search warrant was obtained to search the Elkview residence belonging to ROATSEY. The search warrant was executed on October 28, 2021. During the execution of the search warrant, numerous electronic devices were seized. Among the items

seized was a Samsung tablet consistent with the device that had uploaded the images in the Kik Cybertip. This tablet was found to have been reset to factory settings or otherwise had its contents removed during the week prior to the execution of the search warrant. However, law enforcement was able to determine from a forensic review of the device that the Kik application had previously been present on the device.

12. Many of the devices seized have been forensically reviewed. The review of one such device, a Samsung Android cell phone seized from ROATSEY at the time of the search, and the microSD card contained therein, (collectively, "the Phone") revealed evidence that the following Google accounts had been accessed on the Phone or were associated with websites or applications accessed on the Phone: hiddot1984@gmail.com; therelaxedude84@gmail.com; tmash194@gmail.com; sneakerbox84@gmail.com; cdai28471@gmail.com; hairclub97@gmail.com; docsafecracker@gmail.com; gilliganisland142@gmail.com; costanzag558@gmail.com; yewavery@gmail.com; frankhaney69@gmail.com; ultimatew31@gmail.com; hackneykohen49@gmail.com; cornesdarryl@gmail.com; therock1984z1@gmail.com; and troatsey1@gmail.com (collectively, "the Subject Accounts"). The Phone had evidence showing that it was utilized by ROATSEY, including accessing his email address with his employer, Kanawha County Schools, and regularly receiving text messages from his two sisters and father. The Phone was password protected.

13. As noted above, one of these accounts, ultimatew31@gmail.com, was accessed on the Phone and was also affiliated with the account for which Kik generated the above-described Cybertip. An email located on the Phone was an email from Kik to the ultimatew31@gmail.com email address in which Kik states that the user account is "jsparrow2174." Accordingly, the Phone

and that particular email account are directly connected to the Kik account that was purportedly using to distribute child pornography.

14. Another Google account accessed using the Phone, costanzag558@gmail.com, was used to register an account with Mega, a New Zealand-based company that provides encrypted file-hosting and communications services to the public. As described further below, the Phone revealed that ROATSEY used the Phone to access Mega through an app on his phone and that his Mega account either contained substantial amounts of suspected child pornography or provided ROATSEY with access to substantial amounts of suspected child pornography. Upon request, Mega provided subscriber and other non-content information relating to the Mega account associated with the email address costanzag558@gmail.com. This information indicated that the account was accessed from IP address 47.220.40.206, which is the same IP address identified in the Kik Cybertip and assigned to the residence belonging to ROATSEY.

15. The review of the Phone revealed that ROATSEY utilized screen-recording programs, such as Snapsaver, to make video recordings of all activity that appeared on the screen during the time when the screen-recording program was active. Such activity included movement between apps, scrolling through or clicking on anything within apps, any alerts or banners that appeared on the screen, and any typing done by the user. Many of these recordings indicated that the recordings were documenting the screen of ROATSEY's phone, including alerts for text messages from various family members and screens showing previews of his Kanawha County Schools emails.

16. The review of the Phone located an approximately four-minute video file (the "Subject Video"), created on or about April 29, 2021, that depicted one such screen-recording of ROATSEY's device. The Subject Video depicted the user opening a folder on the Phone labeled

"Productivity." Within this folder was the Mega app. The user opened the Mega app, which displayed numerous folders with names such as "Cp + Rape mixed" and "CP Full." The user accessed several folders and scrolled through dozens of thumbnail previews for videos that could be played by the user (as each video preview had a Play triangle symbol on it). Based solely upon the single frame previewed for each video, the folders contained videos depicting vaginal penetration of toddlers with adult male penises, sado-masochistic bondage of minors, and slight vaginal penetration of what appeared to be an approximately 2- to 3-month-old infant through use of an object.

17. The Subject Video thereafter depicts the user exiting the Mega app and opening another app within the "Productivity" folder, labeled "Cloud Mail.ru."[1] The user again scrolls though a library of video preview thumbnails that appear to depict child pornography. Based upon these single-frame previews, the videos contained depictions of vaginal and anal penetration of numerous infants and toddlers.

18. Next in the Subject Video the user exits the "Cloud Mail.ru" app and the "Productivity" folder. The user opens up an app for his Google Drive account. From the Subject Video, it cannot be determined which of the Subject Accounts was associated with this Google Drive. When opened, the Google Drive account contained four folders: "Sam,"[2] "Child," "Rape," and "Rape1." The "Child," "Rape," and "Rape1" folders each featured an icon on the bottom right corner that indicated the folder was shared with one or more other accounts. The user scrolled

---

[1] Law enforcement has no information indicating that an account with this app is associated with any Google account.

[2] During the Subject Video the user did not access the "Sam" account, and therefore the contents of that folder are unknown. However, SAM is a common acronym for "sexual abuse materials."

through the "Rape," "Rape1," and "Child" folders, which again contained thumbnail previews of videos. The "Rape" folder was shown to contain a video that appears to be entitled "Teacher fucks girls." The Rape1 folder contained a video with a single-frame preview depicting an adult male penis penetrating the vagina of a preteen. The "Child" folder contained still image previews depicting sexually explicit conduct involving minors, including several videos with vaginal penetration of infants and toddlers. The Subject Video ends at this point.

19. The user did not play any of the previewed videos during the Subject Video. During the Subject Video, an alert appeared at the top of the screen indicating that a text message had been received from Terry Roatsey, ROATSEY's father.

20. A review of the Phone also revealed multiple screen recordings of Snapchat conversations with minors, some of whom have been identified by law enforcement as students who attended or were attending Pinch Elementary School, where ROATSEY was employed as the school counselor. These recordings were made starting in January 2020 and proceeding through late summer/early fall of 2020. Rather than using his own identity for the Snapchat account, ROATSEY pretended to be a teenage boy in order to communicate with multiple minors. The Phone contained saved images of the young male that ROATSEY was using as his fictitious Snapchat persona. ROATSEY's fictitious profile utilized the name CDaily, which is similar to the Google account for cdai28471@gmail.com that was accessed by the Phone. At least two of these minors, neither of whom has yet been identified, sent videos of themselves engaged in sexually explicit conduct at ROATSEY's direction. Other minors, some as young as 11 years old, sent videos depicting themselves engaged in sexually suggestive conduct that fell short of the requirements for sexually explicit conduct under federal law.

BACKGROUND CONCERNING GOOGLE[3]

21. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

22. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

23. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

24. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered

---

[3] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

25. Gmail: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

26. Contacts: Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

27. Messaging: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may

also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

28. Google Drive: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive

29. Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to

Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

30. Location History: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

31. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing

history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

32. Google Play: Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

33. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

34. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

35. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects

to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

36. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

37. In my training and experience, evidence of who was using a Google account, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, information from Gmail or Contacts can help to establish the identity of the person using the account; Google Play can identify apps that had been previously downloaded to the phone; Messaging may locate communications between the account owner and individuals with whom they are sharing relevant folders in Google Drive; and Location History can help to identify the user of the account by showing regular activity at their place of employment.

38. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

39. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user

attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

40. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

41. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or potential victims. In addition, emails, instant messages, Internet activity, documents, and contact information can lead to the identification of co-conspirators, victims, and instrumentalities of the crimes under investigation.

42. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including,

but not limited to, information that can be used to identify the account's user or users; the use of applications through which child pornography is stored, shared, or obtained; communications with minors for the purpose of producing child pornography or child erotica; and communication with other individuals involved in the trafficking of child pornography materials.

CONCLUSION

43. Based on the forgoing, I request that the Court issue the proposed search warrant.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Further your Affiant sayeth naught.

SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 21st day of December, 2021.

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA